PCT

WORLD INTELLECTUAL PROP[ERTY ORGANIZATION]
International B[ureau]

INTERNATIONAL APPLICATION PUBLISHED UNDE[R THE PATENT COOPERATION TREATY (PCT)]

WO 9607951A1

(51) International Patent Classification 6 :	A1	(11) International Publication Number: WO 96/07951
G02F 1/1347, H04L 9/08		(43) International Publication Date: 14 March 1996 (14.03.96)

(21) International Application Number: PCT/GB95/02123

(22) International Filing Date: 7 September 1995 (07.09.95)

(30) Priority Data:
PCT/GB94/01952 8 September 1994 (08.09.94) WO
(34) Countries for which the regional or international application was filed: GB et al.
95301050.1 20 February 1995 (20.02.95) EP
(34) Countries for which the regional or international application was filed: GB et al.

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PLC [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

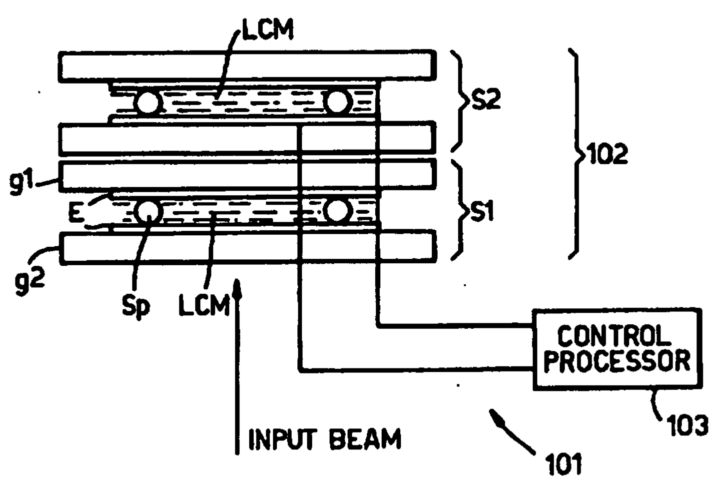
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: KERSHAW, Stephen, Vincent [GB/GB]; 19 Aldercroft Road, Ipswich, Suffolk IP1 6PL (GB). TOWNSEND, Paul, David [GB/GB]; 7 Bramble Drive, Purdis Farm, Ipswich, Suffolk IP3 8ST (GB).

(74) Agent: GILL JENNINGS & EVERY; Broadgate House, 7 Eldon Street, London EC2M 7LH (GB).

(81) Designated States: AU, CA, JP, KR, NZ, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: POLARISATION MODULATION



(57) Abstract

A method of modulating an optical signal includes passing the signal through a liquid crystal modulator thereby modulating the polarisation state. The liquid crystal modulator comprises a plurality of individually switchable liquid crystal cells. These cells are arranged in series between an input and an output of the modulator. The modulator is set in different configurations corresponding to different combinations of settings of the individual liquid crystal cells. It applies one of a multiplicity of discrete polarisation modulation states to the input signal depending upon the configuration chosen. The liquid crystal material may be a ferro-electric material and the modulator may comprise two or three such liquid crystal cells configured, e.g. as half-wave cells or quarter-wave cells. The modulator may be used to modulate a single-photon signal in a method of key distribution using quantum cryptography.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

POLARISATION MODULATION

BACKGROUND TO THE INVENTION

The present invention relates to a method and apparatus for polarisation modulation suitable for use, for example, in an optical communications system in which optical signals are encoded in different polarisation states. It is particularly, but not exclusively, concerned with a communications system employing quantum cryptography for the secure distribution of a key to be used in subsequent encryption/decryption of signals carried by the system.

As described in the present applicant's co-pending International application number PCT/GB 94/01952, quantum cryptography may be carried out using, e.g., modulation of a single-photon signal with different phase or polarisation states. In the case of a system using different polarisation states, it has previously been proposed to use lithium niobate or other crystalline electro-optic modulators. These are birefringent devices which potentially offer high switching rates. However they suffer the significant disadvantages of being expensive to manufacture, and tend to produce high insertion losses. Many lithium niobate devices also suffer from variable frequency response in the lower frequency ranges due to piezo-electric resonances.

SUMMARY OF THE INVENTION

According to a first aspect of the present invention, there is provided a method of modulating an optical signal including passing the signal through a liquid crystal modulator and thereby modulating the polarisation state of the signal, characterised in that in the liquid crystal modulator the signal passes through a plurality of individually switchable liquid crystal cells arranged in series between an input and an output of the modulator, and in that for different input signals, the modulator is set to a different one of a multiplicity of configurations

corresponding to different combinations of settings of the individual liquid crystal cells, thereby applying a corresponding one of a multiplicity of discrete polarisation modulation states to the signal.

The present invention provides a method of modulation which is able to apply a set of discrete polarisation states using relatively simple components with low insertion-loss, namely a stack of liquid crystal cells.

The use of single liquid crystal cells switched between ON and OFF states is of course well known in the field of liquid crystal display devices. It has also been suggested in a few specialised fields of application to use stacks of liquid crystal cells. For example the paper by H.J. Masterson et al published at pp 1249-1251 OPTICS LETTERS, November 15 1989 vol 14 no. 22 describes a Lyot filter which uses a stack of ferroelectric LC cells in combination with a number of birefringent elements to provide a filter whose centre wavelength is switched between two values by having all the LC cells ON or the LC cells OFF. In this application, as in liquid crystal displays, the input and output polarisation states of the transmitted light are determined by polarising filters. In addition further polarisers are required at intermediate stages within the stack of liquid crystal devices to delimit each birefringent segment of the device.

Preferably each liquid crystal cell includes a ferroelectric liquid crystal having a direction of polarisation which switches by 2θ in response to an applied electric control signal, where θ is the characteristic smectic layer tilt angle of the material.

The use of ferroelectric LC materials is preferred as providing cells which are potentially bistable and switched between two discrete states in response to an applied control signal. A series of these cells together with appropriate combinations of control signals can therefore generate the required set of discrete polarisation states.

Preferably the signal modulated by the cell is a single-photon signal and the signal is subsequently detected at a single-photon detector as part of a method of key distribution using quantum cryptography.

The modulator of the present invention was developed in particular to meet the need which arises in quantum cryptography for modulation using sets of discrete polarisation states. The single-photon signal may take the form, for example, of single photons obtained from a parametric optical amplifier source, or, alternatively, may comprise weak pulses of light from an attenuated laser which in general contains no more than one, and on average substantially less than one photon per pulse. Either signal-type exhibits the required quantum properties, and the term "single-photon pulse" is used herein to denote all such signals exhibiting quantum properties, irrespective of how they are produced.

As described in detail in our above-cited co-pending International application, quantum cryptography provides a method for the distribution of a key for use in subsequent encryption/decryption of transmitted data. The security of such a system depends upon the key to the encryption algorithm being available only to authorised users. To this end, the key is distributed over a secure quantum channel carried by single-photon signals and exhibiting non-classical behaviour. The transmitter and the receiver then communicate over a separate channel, known as the public channel, to compare the transmitted and received data. The presence of any eavesdropper intercepting the transmitted single-photon signals encrypted with the key results in a change in the statistics of the received data, which can be detected. Accordingly, in the absence of any such change in the statistics of the data, the key is known to be secure. The secret key thus established can then be used for encryption/decryption of subsequent communications. For added security, the existing key may periodically be replaced by a newly generated key.

A system using quantum cryptography may take any one of a variety of configurations, including those described in our above-cited International application. A multiple-access network may be used for distribution of the key. Optionally, both the transmitter including the source of single photon signals, and the receiver including the single-photon detector may be located at a head-end station connected to such a multiple access network, with subscribers connected to the network being provided with modulators. In such a system the subscribers modulate the single-photon signal which then passes via a looped-back-path to the head-end station for detection.

Although in general quantum cryptography may be carried out using, for example, phase modulation, the present invention is particularly concerned with systems where the key is encrypted on single-photon signals using a modulation alphabet formed from different polarisation states.

Where the modulation alphabet comprises four polarisation states then preferably the modulator comprises two liquid crystal cells arranged in series. Where the four polarisation states comprise four linear states with planes of polarisation which are respectively vertical, horizontal, 45° and 135°, then preferably the two liquid crystal cells are both configured as half wave plates, one cell having a switching angle of θ=22.5°, and the second having a switching angle of θ=11.25°. Alternatively, the four polarisation states may comprise two linear states and two circular states, e.g. linear vertical, linear horizontal, right circular and left circular. In this case, preferably the two cells comprise a half wave cell with a switching angle of θ=22.5°, followed by a quarter wave cell with a switching angle of θ=22.5°.

As a further alternative, the encryption scheme may use six polarisation states formed by a superposition of the two four-state sets discussed above. In this case preferably the modulator comprises three liquid crystal

cells arranged in series, the first and second cells on the input side of the modulator being configured as half wave cells with θ=22.5°, and the third cell on the output side comprising a further half wave cell with θ=11.25°.

According to a second aspect of the present invention, there is provided a modulator for an optical signal including a liquid crystal modulator, characterised in that the liquid crystal modulator comprises a plurality of individually switchable liquid crystal cells arranged in series between an input and an output, and by control means arranged to set the liquid crystal modulator in different ones of a multiplicity of configurations corresponding to different combinations of settings of the individual liquid crystal cells, thereby enabling corresponding ones of a multiplicity of discrete polarisation states to be applied to an optical signal.

According to a third aspect of the present invention there is provided a communications system using quantum cryptography and including a source of single-photon signals, means for modulating the single-photon signals from the source, and means for detecting the modulated signals, characterised in that the means for modulating the single-photon signals comprise a modulator in accordance with the second aspect of the present invention.

<u>BRIEF DESCRIPTION OF THE DRAWINGS</u>

Systems embodying the present invention will now be described in further detail, by way of example only, with reference to the accompanying drawings in which:

Figure 1 is a schematic of a polarisation modulator embodying the present invention;

Figure 2 is a diagram illustrating the general case of a stack of n liquid crystal cells;

Figure 3 is a diagram illustrating the electric field induced reorientation of molecules in a ferro-electric liquid crystal material shown in bistable states before and after switching;

Figure 4 shows a first example of a quantum cryptography network;

Figure 5 shows a second example of a quantum cryptography network; and

Figure 6 is a flow diagram for the operation of the network of Figure 4.

DESCRIPTION OF EXAMPLES

A polarisation modulator 101 comprises a stack 102 of liquid crystal cells. In the example of Figure 1, the stack comprises two chiral smectic-C cells S1, S2. Each cell comprises a pair of glass substrates g1, g2 with an ITO electrode E formed on each substrate. The thickness of the ITO electrode is chosen to provide a resistivity of around 50 Ohms/square. Appropriate pre-coated ITO electrodes are available commercially in the UK from Balzers. A polyimide coating, rubbed in one direction is formed on each of the electrodes. The rubbing directions on top and bottom substrates are usually opposed to minimise the stored splay elastic energy arising from the slight surface pretilt of the liquid crystal molecules. Although polyimide alignment layers are preferred, other planar alignment materials are possible e.g. rubbed nylon, rubbed polyvinyl alcohol, or obliquely evaporated silicon oxide or magnesium fluoride. On balance polyimides have so far tended to give the best all round performance. The polyimide coating may have a thickness in the range 0.1 to 0.2 microns. By contrast, the alternative inorganic coatings referred to above may have thicknesses in the range 200 to 500 Angstroms.

As an alternative to the structure of Figure 1, a single double-sided substrate may replace the upper substrate of S1 and the lower substrate of S2. A control processor 103 sets the state of the modulator 101.

Spacers SP separate the substrates and define a volume in which the liquid crystal material is confined. Spacer material may be located at the periphery or scattered, possibly randomly throughout the cell. An adhesive seal

may be applied to one of the substrates to define the lateral boundary of the cell. The seal will have one or more gaps to permit capillary filling (under vacuum if only one gap is used) with liquid crystal. There is a wide range of ferroelectric liquid crystal (FELC) and liquid crystal mixtures available commercially that may be used in such devices, for example a suitable material is that available from Merck as ZLI-4318. A complete listing of available ferroelectric mixtures is available from Merck Ltd. at Merck House, Poole, Dorset, BH15 1TD, UK.

The spacing between the glass substrates in each cell is typically in the range 1.5 to 3μm. The thickness of each cell and refractive index anisotropy of the liquid crystal is chosen so that at the wavelength of the input beam the cell functions e.g. as a half-wave or quarter-wave plate. In the present example, the liquid crystal material is assumed to have a typical birefringence of 0.15. Therefore, for operation at a wavelength of 830mn, for operation as a half-wave plate the cell is arranged to have a thickness of 2.8μm, while a quarter-wave plate uses a cell of half that thickness.

If the liquid crystal material has a different birefringence, then the cell thickness is scaled accordingly. Selected FELC materials may have birefringences as high as 0.5. However, more typically, FELCs have birefringences in the range 0.15-0.13 at 589nm. When a field is applied across each cell using the electrodes, the liquid crystal molecules in the cell tilt at a characteristic tilt angle θ as shown in Figure 3. Changing the polarity of the applied field flips the molecules through an angle of 2θ. The cell functions as a bistable device which is switched by the field between these two stable orientation states and can not in general have any stable intermediate orientations. Ferro-electric chiral smectic C materials possess a strong spontaneous polarisation at an angle approaching 90° to the longitudinal direction of the molecule. It is this

spontaneous polarisation that interacts with the electric field. The surface stabilisation and the chirality of the material ensures that when the spontaneous polarisation reverses during switching, then the layer tilt flips from $+\theta$ to $-\theta$ in the plane orthogonal to the applied electric field. The magnitude of the layer tilt is not altered by the field, but only its rotation sense. It should be understood that there is no tendency for the longitudinal axis of the molecules to line up with the electric field, i.e. for them to tilt relative to the cell walls. The layer tilt is always induced in the plane along the field direction. Bistable FE switching can be observed at voltages typically up to +/- $50V\mu m^{-1}$ or more before they break down.

In Figure 3 the dotted lines separate smectic layer planes, and the solid slanted lines mark the molecular axes.

Figure 2 shows schematically a stack of LC devices (1-n) for polarisation state control. The optic axis of each cell is at an angle ϕ_i (where i=1 to n). to the horizontal axis. The input polarisation state can be described by the Jones vector.

$$Linear = \begin{bmatrix} Cos(\phi) \\ Sin(\phi) \end{bmatrix} \tag{1}$$

For each device there is an associated Jones matrix which acts on the input vector in sequence. A half wave plate has the vector.

$$Half\ Wave\ Plate = i\begin{bmatrix} -Cos(2\phi) & -Sin(2\phi) \\ -Sin(2\phi) & Cos(2\phi) \end{bmatrix} \tag{2}$$

whilst a quarter wave plate is described by the matrix,

$$Quarter\ Wave\ Plate = \frac{1}{\sqrt{2}}\begin{bmatrix}1+i(Cos^2\phi - Sin^2\phi) & 2iCos\phi Sin\phi \\ 2iCos\phi sin\phi & 1+i(Cos^2\phi - Sin^2\phi)\end{bmatrix} \quad (3)$$

The output polarisation state $\underline{O}$ after passing through a series of devices each with matrix $\underline{M}_i$ is then $\underline{O}=\underline{M}_1 \cdot \underline{M}_2 \cdot \underline{M}_3 \cdot \underline{I}$. If the resulting vector has the form of equation (1) the output is linearly polarised. Circularly polarised outputs have the form

$$Right\ Circular = \frac{1}{\sqrt{2}}\begin{bmatrix}1 \\ -i\end{bmatrix}$$

or

$$Left\ Circular = \frac{1}{\sqrt{2}}\begin{bmatrix}1 \\ i\end{bmatrix}$$

The properties outlined above enable a stack of switched cells such as that shown in Figure 1 to function as a polarisation modulator for selecting predetermined discrete polarisation states. For example, there has been described in our above-cited International application a modulation scheme using four linear polarisation states of 0°, 90°, 45°and 135°. To implement this scheme, the first cell S1 is arranged to have a switching angle of θ=22.5° and the second cell S2 is arranged to have θ=11.25°. It is assumed that when both cells are in state "0" that their optical axis are parallel. Labelling the two states of the first cell as 0 and $\pi/4$, and the two states of the second cell as 0 and $\pi/8$, the different outputs required from the polarisation modulator are obtained as show in Table 1 below:

TABLE 1

Input	cell 1 state	cell 2 state	Output

linear vertical	0	0	linear vertical
linear vertical	$\pi/4$	0	linear horizontal
linear vertical	0	$\pi/8$	linear 135° to horizontal (ccw)
linear vertical	$\pi/4$	$\pi/8$	linear 45° to horizontal (ccw)

An alternative encoding scheme might use two linear polarisation states and two circular polarisation states - linear vertical, linear horizontal, right circular and left circular. A liquid crystal modulator for implementing such a scheme again comprises a stack of two cells. In this case the first cell S1 is a half-wave cell with θ=22.5° and the second cell S2 is a quarter-wave cell with θ=22.5°. The following table shows the different states for this modulator:

TABLE 2

Input	cell 1 state	cell 2 state	Output
linear vertical	0	0	linear vertical
linear vertical	0	$\pi/4$	right circular
linear vertical	$\pi/4$	$\pi/4$	left circular
linear vertical	$\pi/4$	0	linear horizontal

A further alternative encoding scheme comprises six states being a superposition of the states used in the

first two schemes. A modulator to implement this scheme uses a stack of three cells, the first two cells being as described in the immediately preceding example, and being followed by a third cell which is a half-wave cell with θ=11.25°. The states for this modulator are shown in the following table:

TABLE 3

Input	cell 1 state	cell 2 state	cell 3 state	output
linear vertical	0	0	0	linear vertical
linear vertical	$\pi/4$	0	0	linear horizontal
linear vertical	0	0	$\pi/8$	linear 135°
linear vertical	$\pi/4$	0	$\pi/8$	linear 45°
linear vertical	0	$\pi/4$	0	left circular
linear vertical	$\pi/4$	$\pi/4$	0	right circular
linear vertical	0	$\pi/4$	$\pi/8$	left circular
linear vertical	$\pi/4$	$\pi/4$	$\pi/8$	right circular

In this example, the left circular pair are essentially degenerate, as are the right circular pair. While the absolute phase of each of the circular polarisations in each pair differs, the fact that the intensity is time averaged over a period many times the oscillation period of the wave means that the absolute phase is irrelevant. One is therefore left with four linear polarisation states and a left and right circular

polarisation state. Effectively, when cell 2 is on, it does not matter what state cell 3 is in.

A number of other configurations are possible for a stacked liquid crystal modulator. For example the half-wave cells in the examples described above could be split into pairs of quarter-wave cells. The order of some of the cell combinations could also be changed. A further possible modification is the use of electroclinic devices to provide continuously tunable wave plates providing further coding flexibility. The term electroclinic is used to denote chiral smectic A liquid crystals which have a continuously variable molecular layer tilt angle, the angle being linearly dependent on the cell drive voltage. Again, electroclinic materials are available commercially such as 764E, 854E, etc from Merck Ltd.

The use of liquid crystal modulators as described above is found to be highly advantageous, enabling switching at relatively high rates with, for example, 10μs pulse spacing and offering the possibility of compact, cheap devices.

Figure 4 shows a specific example of a broadcast network containing two receivers and a transmitter. The transmitter consists of a gain-switched semiconductor laser 9, which may be a DFB or Fabry-Perot device, an attenuator or intensity modulator 7, and a polarisation modulator 8 and control electronics 10. The single-photon detectors in the receivers may be avalanche photodiodes (APDs) biased beyond breakdown and operating in the Geiger mode with passive quenching, as discussed in P. D. Townsend, J. G. Rarity and P. R. Tapster, Electronics Letters, 29, 634 (1993). Silicon APDs such as the SPCM-100-PQ (GE Canada Electro Optics) can be used in the 400-1060 nm wavelength range, while Germanium or InGaAs devices such as the NDL5102P or NDL5500P (NEC) can be used in 1000-1550 nm range. Each receiver includes a microprocessor control unit 2, which receives the output of the APD via a discriminator/amplifier circuit 3. The control unit 2 also

controls an electronic filter 4 and local oscillator 5, as well as the APD bias supply 6. The electronic filter 4 isolates the first harmonic of the frequency spectrum of the signal output by the APD in response to synchronising pulses received via the network. This generates a sinusoidal signal at the pulse frequency which locks the local oscillator 5. The output of the local oscillator 5 is received at the control unit 2 to provide a timing reference during quantum transmissions.

The use of multi-photon signals on the transmission medium to calibrate the system prior to or during quantum transmission is described in further detail in our co-pending International patent application PCT/GB93/02637, the contents of which are incorporated herein by reference. This makes it possible to compensate, e.g., for changes in fibre polarisation resulting from environmental effects. In use, in an embodiment where timing information is not transmitted concurrently with quantum transmissions, key distribution is initiated by the transmitter sending a stream of timing pulses into the network. These are bright, multi-photon pulses. Accordingly these pulses behave classically, and are received by both of the terminals connected to the network. During this phase the receivers may set the reverse bias on their single-photon detectors to be well-below breakdown so that internal gain is low. In this mode the APDs can detect the multi-photon timing pulses without suffering from saturation. Each APD output signal then contains a frequency component at the fundamental repetition rate of the pulsed source, and this is used to lock the local oscillator in the receiver as described above.

Subsequently the optical source in the transmitter is set to produce single-photon signals, for example by connecting an attenuator in line with a multi-photon source. The output pulses from the transmitter then contain on the order of 0.1 photons on average. In the receivers, the APDs are biased beyond breakdown so that

internal gain is high enough to achieve detection sensitivity at the single-photon level. Then, as shown in the flow diagram of Figure 6, encoded pulses are sent from the transmitter onto the network using, e.g., one of the encoding alphabets described above. After a sufficient number of single photon pulses have been transmitted for each of the receivers to establish the required number of key bits, a public discussion phase is entered in which the transmitter and receivers communicate on a public channel provided, for example, by the transmission of multi-photon signals on the network. The sent and received sequences are compared, data for time slots in which different encoding/measurement bases were used discarded, and error correction carried out. After error correction, any residual discrepancy in the transmitted and received data is compared with a predetermined threshold. If the discrepancy level is acceptably low, then the shared data sequences are known to be secure and are used to provide a shared secret key. The key is then available for subsequent encryption/decryption of data transmissions between the transmitter and receivers.

The polarisation modulator of the present invention may be used in a variety of different network topologies. For example, Figure 5 shows a quantum cryptographic system in which the receivers, rather than detecting the photon destructively, modulate it and pass it back to the head-end station or "controller". This approach is described in further detail in our pending International application PCT/GB93/02637. A possible attack upon such an implementation requires an eavesdropper to intercept the quantum channel on both sides of a given user Bob. Then by transmitting and detecting a multi-photon signal, Eve (the eavesdropper) can determine unambiguously the state of Bob's modulator. In practice however it is likely to be very difficult for Eve to establish connections to two or more points in the network. Nonetheless, where it is desired to protect against an attack of this type, this may

be done by providing at least one of the receivers of the network with a photodetector connected to the network by a relatively weak tap. This photon detector need not be of the sensitivity of the single-photon detectors employed conventionally in receivers, nor need every user have such a detector. The presence of such a detector in the network facilitates the detection of any multi-photon probe used by Eve.

CLAIMS

1. A method of modulating an optical signal including passing the signal through a liquid crystal modulator and thereby modulating the polarisation state of the signal, characterised in that in the liquid crystal modulator the signal passes through a plurality of individually switchable liquid crystal cells (S1,S2) arranged in series between an input and an output of the modulator, and in that for different input signals, the modulator is set to different ones of a multiplicity of configurations corresponding to different combinations of settings of the individual liquid crystal cells, thereby applying a corresponding one of a multiplicity of discrete polarisation modulation states to the signal.

2. A method according to claim 1, in which each liquid crystal cell (S1,S2) includes a ferro-electric liquid crystal material and the direction of alignment of the optic axis of the liquid crystal cell switches by 2θ in response to an applied electric control signal, where θ is the characteristic tilt angle of the material.

3. A method according to claim 1 or 2, in which the signal modulated by the cell is a single-photon signal and the signal is subsequently detected at a single-photon detector as part of a method of key distribution using quantum cryptography.

4. A method according to claim 3, in which the modulation alphabet comprises four polarisation states and the polarisation modulator comprises two liquid crystal cells arranged in series.

5. A method according to claim 4, in which the modulation alphabet comprises four polarisation states at 0°, 45°, 90°, 135° to a reference axis and the polarisation modulator comprises two liquid crystal cells both configured as half-wave plates.

6. A method according to claim 4, in which the four polarisation states comprise two linear states and two

circular states and the polarisation modulator comprises a half-wave cell and a quarter-wave cell arranged in series.

7. A method according to claim 4, in which the modulation alphabet comprises six polarisation states including linear polarisation states and left and right circular polarisation states, and the modulator comprises three liquid crystal cells arranged in series.

8. A method according to claim 7, in which the three liquid crystal cells comprise two half-wave cells, these having a tilt angle θ substantially equal to 22.5°, and a third cell being a quarter-wave cell having a tilt angle θ substantially equal to 11.25°.

9. A modulator for an optical signal including a liquid crystal modulator (101), characterised in that the liquid crystal modulator comprises a plurality of individually switchable liquid crystal cells (S1,S2) arranged in series between an input and an output, and by control means (103) arranged to set the liquid crystal modulator in different ones of a multiplicity of configurations corresponding to different combinations of settings of the individual liquid crystal cells (S1,S2), thereby enabling corresponding ones of a multiplicity of discrete polarisation states to be applied to an optical signal.

10. A modulator according to claim 9, in which each liquid crystal cell (S1,S2) includes a ferro-electric liquid crystal material (LCM) having an optic axis which switches by 2θ in response to an applied electric control signal, where θ is the characteristic tilt angle of the material.

11. A modulator according to claim 9, in which one or more of the liquid crystal cells includes a chiral smectic A (Electroclinic) liquid crystal, the orientation of the optic axis of the cell being drive-voltage-dependent.

12. A communications system using quantum cryptography and including a source of single-photon signals (7,9), means (8) for modulating the single-photon signals from the source, and means (ADD) for detecting the modulated signals, characterised in that the means (8) for modulating

the single-photon signals comprise a modulator according to any one of claims 9 to 11.

Fig.1.

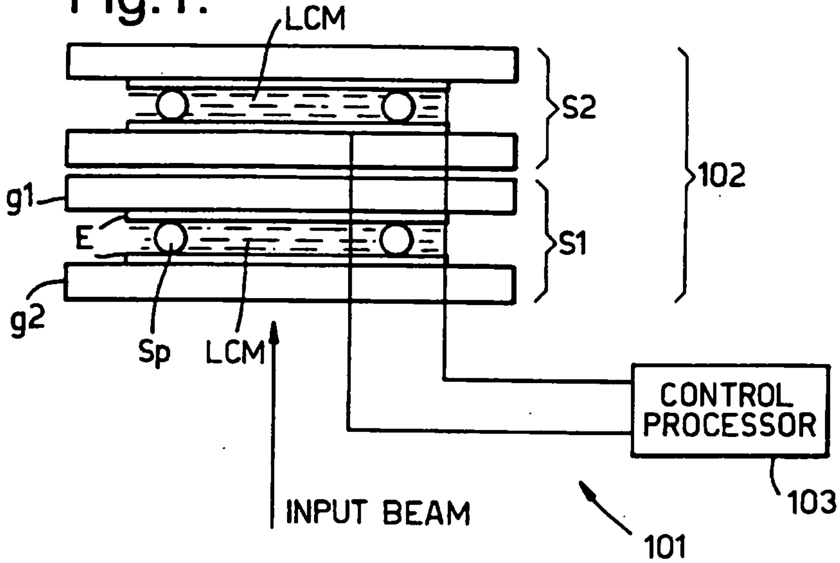


Fig.2.

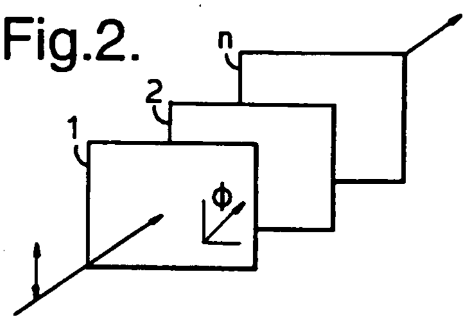


Fig.3.

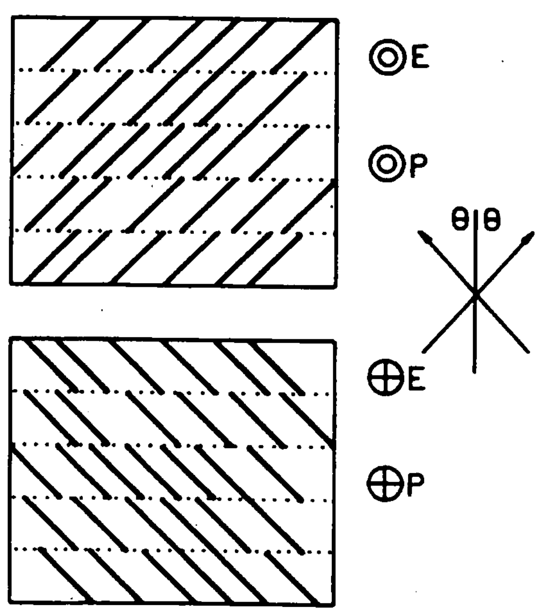


Fig.4.

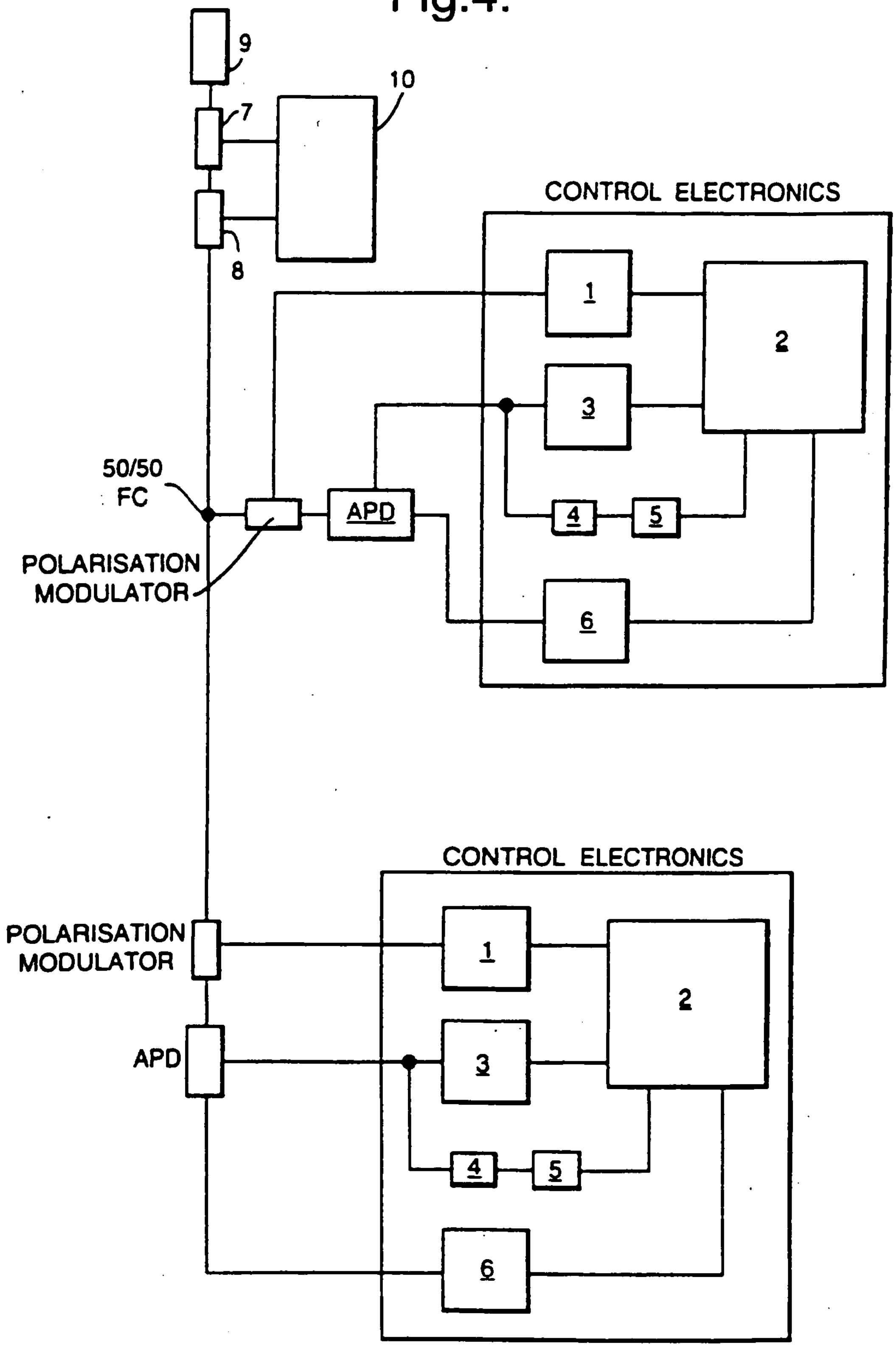

9
10
7
8
CONTROL ELECTRONICS
1
2
3
50/50
FC
APD
4
5
POLARISATION
MODULATOR
6
CONTROL ELECTRONICS
POLARISATION
MODULATOR
1
2
APD
3
4
5
6

Fig.5.

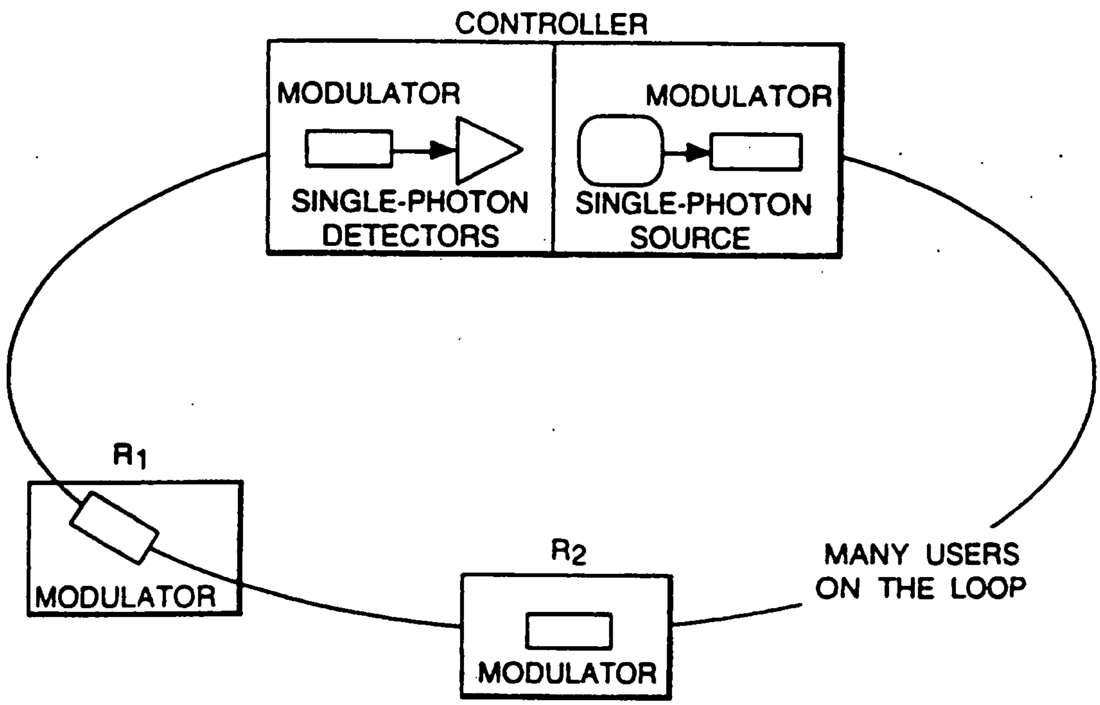
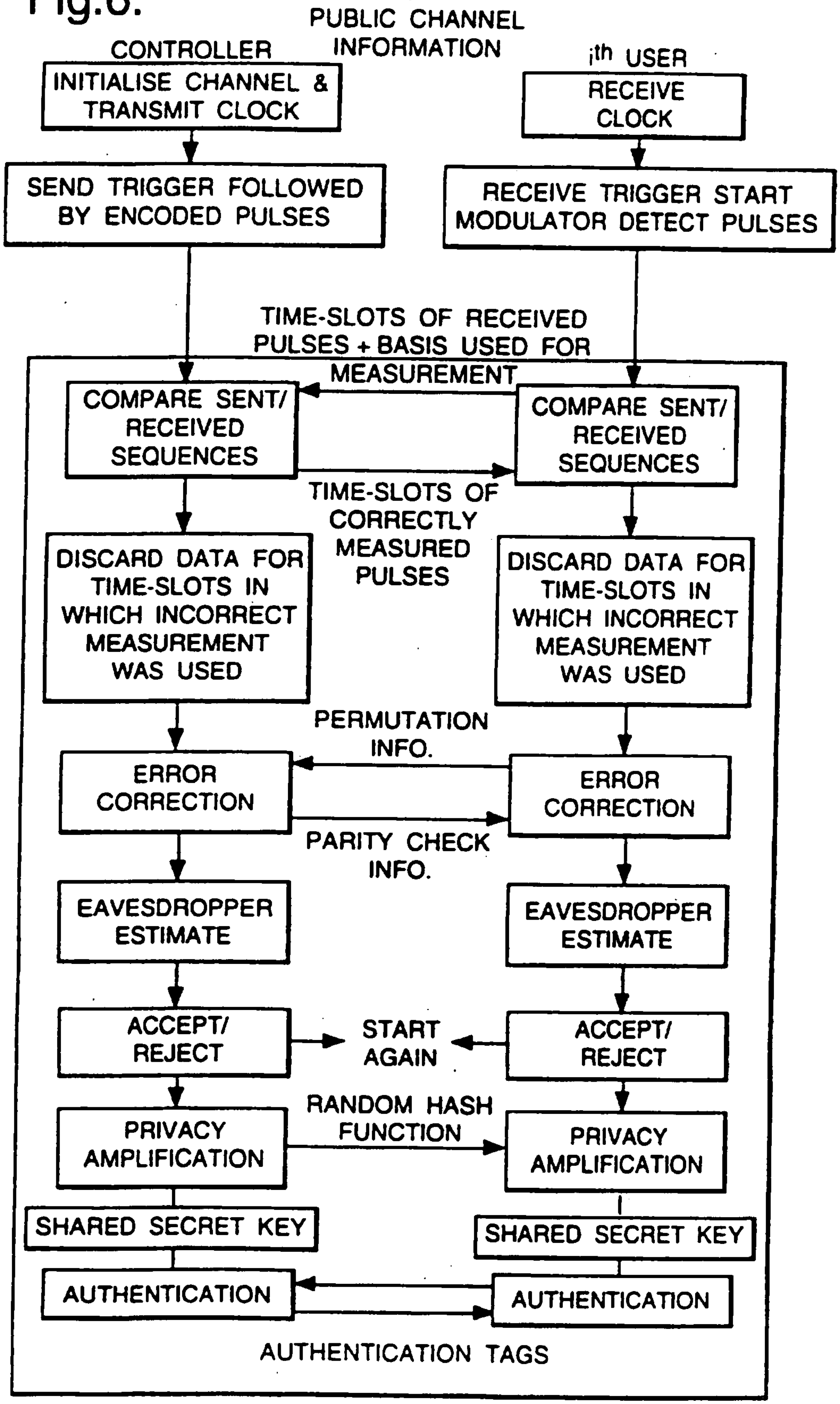

CONTROLLER
MODULATOR
MODULATOR
SINGLE-PHOTON
DETECTORS
SINGLE-PHOTON
SOURCE
R1
MODULATOR
R2
MODULATOR
MANY USERS
ON THE LOOP

Fig.6.


PUBLIC CHANNEL INFORMATION
CONTROLLER
INITIALISE CHANNEL & TRANSMIT CLOCK
SEND TRIGGER FOLLOWED BY ENCODED PULSES
ith USER
RECEIVE CLOCK
RECEIVE TRIGGER START MODULATOR DETECT PULSES
TIME-SLOTS OF RECEIVED PULSES + BASIS USED FOR MEASUREMENT
COMPARE SENT/ RECEIVED SEQUENCES
COMPARE SENT/ RECEIVED SEQUENCES
TIME-SLOTS OF CORRECTLY MEASURED PULSES
DISCARD DATA FOR TIME-SLOTS IN WHICH INCORRECT MEASUREMENT WAS USED
DISCARD DATA FOR TIME-SLOTS IN WHICH INCORRECT MEASUREMENT WAS USED
PERMUTATION INFO.
ERROR CORRECTION
ERROR CORRECTION
PARITY CHECK INFO.
EAVESDROPPER ESTIMATE
EAVESDROPPER ESTIMATE
ACCEPT/ REJECT
START AGAIN
ACCEPT/ REJECT
RANDOM HASH FUNCTION
PRIVACY AMPLIFICATION
PRIVACY AMPLIFICATION
SHARED SECRET KEY
SHARED SECRET KEY
AUTHENTICATION
AUTHENTICATION
AUTHENTICATION TAGS

INTERNATIONAL SEARCH REPORT

Inter   nal Application No
PCT/GB 95/02123

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G02F1/1347 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G02F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,90 09614 (LAGERWALL SVEN T) 23 August 1990 see abstract see page 1, line 23 - page 2, line 14 see page 4, line 25 - page 5, line 5 see page 7, line 37 - page 8, line 18 see claims 1,2,10,11; figures 5,6,10 see figures 5,6,10	1,2,9-11
Y	idem	3-8,12

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 December 1995	22.12.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Iasevoli, R

Inte nal Application No
PCT/GB 95/02123

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JOURNAL OF APPLIED PHYSICS, 15 NOV. 1989, USA, vol. 66, no. 10, ISSN 0021-8979, pages 4983-4995, XP 000105101 ANDERSSON G ET AL 'Device physics of the soft-mode electro-optic effect' see section VI, paragraphs 1-3,6 see figures 6,8,9	1,2,9-11
A	idem	4-8

X	WO,A,88 06303 (GEN ELECTRIC CO PLC) 25 August 1988 see abstract; claims; figures 1,9,12	1,9

Y	WO,A,94 15422 (BRITISH TELECOMM ;TOWNSEND PAUL DAVID (GB)) 7 July 1994 see abstract see page 13, line 11 - line 29 see claims; figure 6	3-8,12

P,X	APPLIED OPTICS, 10 FEB. 1995, USA, vol. 34, no. 5, ISSN 0003-6935, pages 832-837, XP 000489988 NAKAGAMI T ET AL 'Ferroelectric liquid-crystal polarization-control devices with a double-layer cell structure' see the whole document	1,2,9,10

P,X	PATENT ABSTRACTS OF JAPAN vol. 95 no. 003 & JP,A,07 077699 (FUJITSU LTD) 20 March 1995, see abstract	1,2,9,10

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. al Application No
PCT/GB 95/02123

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9009614	23-08-90	EP-A-	0409975	30-01-91
		JP-T-	3505013	31-10-91
WO-A-8806303	25-08-88	DE-A-	3881780	22-07-93
		DE-T-	3881780	07-10-93
		EP-A,B	0302091	08-02-89
		GB-A,B	2202643	28-09-88
		JP-T-	1502462	24-08-89
		US-A-	5005952	09-04-91
WO-A-9415422	07-07-94	AU-B-	5709994	19-07-94
		AU-B-	7543894	27-03-95
		AU-B-	7543994	27-03-95
		AU-B-	7544094	27-03-95
		AU-B-	7544194	27-03-95
		CA-A-	2152628	07-07-94
		EP-A-	0676110	11-10-95
		WO-A-	9507582	16-03-95
		WO-A-	9507583	16-03-95
		WO-A-	9507584	16-03-95
		WO-A-	9507585	16-03-95